UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/675,652	09/30/2003	Jeyhan Karaoguz	15046US01	5798

23446 7590 08/05/2008

MCANDREWS HELD & MALLOY, LTD
500 WEST MADISON STREET
SUITE 3400
CHICAGO, IL 60661

EXAMINER
POLTORAK, PIOTR

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
08/05/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/675,652	KARAOGUZ ET AL.	
	Examiner	Art Unit	
	PETER POLTORAK	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 May 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) _____ is/are rejected.

7)☒ Claim(s) *8 and 25* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 5/12/08 has been entered.

Response to Arguments/Amendments

2. Applicant's arguments have been carefully considered.

   In light of applicant's amendments and amendments the objections, and 112 paragraph rejections, cited in the previous Office Action are withdrawn.

3. As per claim 1, 11 and 18, based on the fact that "information that enables billing of the user... is related to the user, rather than to the STB45", applicant argues that Handelman does not disclose "searching by the node" for a previously acquired security data associated with a location of previous operation of the media peripheral".

4. Applicant's argument has been carefully considered but was not found persuasive. An ordinary artisan in the art of billing would recognize that including an address of the subscriber (e.g. home address at which the subscriber operates the media peripheral) in the billing information, if not inherent, it would have been an obvious variation given the benefit of enabling the billing information delivery to the subscriber (see Juneau, USPUB 2002/0019739, for example).

5. Claims 1-28 have been examined.

   The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 102

6. Claims 11-17 are rejected under 35 U.S.C. 102(e) as anticipated by or, in the alternative, under 35 U.S.C. 103(a) as obvious over Paila (USPN 2004/0072557).

   As per claims 11-13, Paila discloses a method for establishing secure access to a media peripheral (MN) via a node (ATT) in a communication network (see Fig. 1, for example).

   In Fig. 3 (and associated text) Paila discloses facilitating secure communication between the media peripheral and the communication network (Paila, [0053-0055]) that includes detecting by the node when the media peripheral is communicatively coupled to the node (action A2 and associated text, for example), utilizing acquired by the node, upon said detection, security data associated with the media peripheral (M2 includes MN_NAI identifying MN, the home domain and authority AAAH, for example, Paila, [0037-0040]) and utilizing security data associated with the node (e.g. the AAAL must receive at least some identification of ATT; otherwise sending data back to ATT, as indicated by the disclosure of step A8 would not be possible).

7. Paila does not explicitly disclose that the security data is associated with location of previous operation of the media peripheral. However, the main purpose of portable devices (such as media peripherals disclosed by Paila) is to operate within the home

domain. Thus, operating the peripheral in peripheral's home domain preceding operating the peripheral in a foreign domain (equating the security data comprising MN_NAI value to "a location of the previous operation of the media peripheral"), if not inherent, would have been at least implicit.

8. As per claim 14, Paila discloses transferring said security data to a media exchange server (AAAL) coupled to the communication network (action A3).
9. As per claim 15, Paila discloses authenticating the acquired security data utilizing the security data associated with the node (Paila, action A4).
10. As per claim 16, Paila's disclosure of "attendant merely allows the mobile node's traffic to pass the attendant from this moment on" in paragraph [0053]) inherently includes registering the media peripheral for subsequent operation in the communication network. Otherwise, attendant would not be able to "recognize" the mobile node and the process of authorization would have to be repeated.
11. However, even if somehow Paila's disclosure was implemented without registering, registering devices for subsequent operations are old and well known in the art of the networking (stateful firewalls, DHCP, etc.), and it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate registering the media peripheral for subsequent operation given the benefit of efficiency and fault avoidance.
12. As per claim 17, distributing data for said registered media peripheral via one or both of the node and at least another media peripheral in the communication network (Paila, action A9, for example).

13. Claims 1-3, 6, 10-13, 18-20, 23 and 27-28 are rejected under 35 U.S.C. 102(e) as anticipated by Birell (USPN 5805803).

Birrell discloses acquiring by the node (Tunnel 140) security data associated with the media peripheral (a request for a secure service received from client 110, Birrell, col. 3 lines 61-col. 4 line 12, for example).

14. As per claims 1, 3, 11, 13, 18 and 20, in col. 3 line 61-col. 4 line 12, Birrell discloses as follows:

> "During operation of the arrangement 100, a user of the client computer 110 makes a connection, via the network 120, with the tunnel 140 using a public Internet service provider (ISP) such as AT&T (.TM.) or Earthlink (.TM.). Alternatively, a computer connected to the Internet at a "cyber-cafe" such as Cybersmith (.TM.) can be used. Many other connection mechanisms can also be used.
>
> FIG. 2 and 3 shows the exchange of messages 200 which occur between the client computer 110, and the components of the tunnel 140 and the resources of the intranet 150 after the connection has been established.
>
> Initially, the user specifies a private intranet resource to be accessed using the browser 111 of the client 110. The location of the private resource is specified using a URL. The public request 310, e.g., "get http://M/P," to access the resource is communicated to the redirector 142 in a message 201 using the non-secure (public) protocol HTTP. The notation "M/P" indicates some resource such as a server, file, Web page, mail message, or the like."

This reads on acquiring by the node (Tunnel 140) security data associated with the media peripheral (a request for a secure service received from client 110).

In col. 4 lines 18-27 Birrell discloss:

> "(13) At this point, if the client 110 is already known to the proxy server, then proceed with message 209, i.e., request 370 below. Otherwise, in the case where the client is unknown, the

redirected browser makes a secure request 330 in a message 203 to the proxy server 143 for the desired resource. In the case, where the client 110 is unknown, the proxy server 143 replies a message 204 to demand that the user makes an authentication request 205 using the checker 141, e.g., a redirect 340 to the checker 141."

This reads on: "searching by the node, for a previously acquired security data" associated with a location of previous operation of the media peripheral

The above Birell's disclosure with teaching in col. 4 lines 27-36:

(14) In response to the request 205, the checker 141 sends a form 206 to the client computer 110 to allow the user to supply authentication information, for example, a user name and password. User identification (ID) is replied (350) in message 207. Alternatively, a secure challenge-response authentication can be performed with a cryptographic device, such as a cryptokey or smart card, in the user's possession. The name and password can be verified against a user database maintained inside the firewall 130."

reads on: "if said previously acquired security data is not found, exchanging between the node and the media peripheral information associated with the media peripheral, while the media peripheral is located in the home".

Similarly, col. 4 lines 18-27 with

"As a result of the interchanges with the checker 141, the client computer can be provided, in step 360, a validation token 299 in message 208. The token can be in the form of an X.500 certificate. Alternatively, the token 299 can be a short-term password to authenticate the user on the HTTPS connection. The short-term password might automatically get installed in the client 110 as a Web "cookie" as a side-effect of the interchange. The message 208 also redirects the browser 111 to further communicate with the proxy server 143.

Therefore, in a next message 209, the client send the request for the resource plus the token 299 to the proxy server 143. When the proxy server 143

> receives the message, it validates the token 299. If the token is valid, then the proxy server 143 behaves as a conventional proxy server.
>
> The proxy server 143 forwards the authenticated request 210 to the specified resource 160 inside the firewall 130 using the non-secure HTTP protocol. The resource 160 replies to the request with, for example private data, in message 211. The proxy server 143 then forwards the data, using secure HTTPS protocol, in a message 212 (step 380).
>
> Subsequent requests for private resources during the session can be handled as follows. The resource is specified in a public message 201 to the redirector 142. The redirector replies message 202. The client 110 now in possession of the token 299 replies message 208 (step 370) causing the further interchange of message 210-212 between the proxy and the server controlling the private resource 160. "

as taught in col. 4 lines 37-64, reads on: "if said previously acquired security data is found: utilizing by the node, said acquired security data associated with the media peripheral and said previously acquired security data to facilitate secure communication between the media peripheral in the home and the communication network".

15. As per claims 2, 6, 10, 12, 19, 23 and 27-28, Birell discloses that the security data could be a digital certificate (e.g. col. 4 lines 37-40), if previously acquired security data associated with the media peripheral is found, acquiring at least one identifier associated with a location of previous operation of the media peripheral (e.g. col. 4 lines 47-57) and that the exchanged information comprises a previously established password (Birell, col. 4 lines 34-35).

Claim Rejections - 35 USC § 103

16. Claims 1-4, 6-7, 10-13, 18-21, 23-24 and 27-28 are rejected under 35 U.S.C. 103(a) as obvious over Birell (USPN 5805803).

Birell's disclosure has been discussed above.

17. Note that a message 209 sent from the peripheral to the node disclosed in col. 4 line 47-49 could also be interpreted as an acquired secure data associated with the media peripheral and validating the token 299 disclosed in col. 4 lines 49-51. The process of token validation would have inherently involve searching by the node, for a previously acquired security data associated with a location of previous operation of the media peripheral, and Birell's disclosure in col. 4 lines 50-64 evidences utilizing by the node, the acquired security data associated with the media peripheral and the previously acquired security data to facilitate secure communication between the media peripheral in the home and the communication network.

18. Birell's disclosure discusses only the successful authentication of a token within a message and does not address the situation when the token authentication fails. As a result, in this interpretation, Birell does not disclose that if the previously acquired security data is not found the node and the media peripheral information exchange information (such as a previously established password).

However, configuring the system to exchange information between the node and the media peripheral if a transaction fails (e.g. the previously acquired security data is not found) is old and well known in the art of computer authentication (as also disclosed by Birell in col. 4 lines 23-36) and would have been an obvious variation to an ordinary artisan given the benefit of enabling an additional authentication.

19. As per claims 4 and 2, in this interpretation of Birell's disclosure, the proxy server 143 in the tunnel 140 reads on an exchange media server authenticating the acquired security data.

20. As per claims 6-7 and 23-24, Birell's disclosure of forwards the authenticated request to the specified resource in col. 4 lines 52-58 evidences acquiring at least one identifier based on the previously acquired security data associated with a location of previous operation of the media peripheral.

21. Claims 1, 3, 6-7, 11-13, 18, 20 and 23-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Handelman (USPub 2004/0016002).

As per claims 1, 6-7 ,18 and 23-24, Handelman discloses at least one processor (an system processing a client request, e.g. a system comprising headend that includes Hardware Configuration Provider Unit 70, Fig. 1 or 2) that acquires security data (a representation of financial transaction details and/or a payment identification code that may be processed to enable billing of the user, [0095]) associated with the media peripheral (STB 45); said at least one processor searches for a previously acquired security data associated with a location of previous operation of the media peripheral (the headend then processes the payment identification code to bill the user [0095] clearly discloses that the headend must have some previously acquired security data corresponding to the security data. As per location, the examiner points out that in addition to some kind of address present in the previously acquired security data, which must be present for the user to receive billing data, which reads "a previously acquired security data being "associated" with a location of previous

operation of the media peripheral, some kind of location of the equipment must be present in the system in order for the Hardware Configuration Provider Unit to be able to receive data). Handelman discloses that if said previously acquired security data is found, said at least one processor utilizes said acquired security data associated with the media peripheral and said previously acquired security data to facilitate secure communication between the media peripheral in the home and the communication network, after successful processing of the data (a successful transaction, *which inherently would involve at least associating and comparing the acquired security data and the previously acquired security data*, results in data being communicated to the media peripheral, e.g. [0099]).

22. Although Handelman does not explicitly disclose that the billing information is associated with an address of the user operating the media peripheral (the user's address). However, an ordinary artisan in the art of billing would recognize that including an address of the subscriber (e.g. home address at which the subscriber operates the media peripheral) in the billing information, if not inherent, it would have been an obvious variation given the benefit of enabling the billing information delivery to the subscriber (see Juneau, USPUB 2002/0019739, for example).

23. Handelman does not disclose exchanging between the node and the media peripheral information associated with the media peripheral if said previously acquired security data is not found.

However, Handelman discloses generating a message indicating a successful transaction ([109]) and an ordinary artisan would readily recognize the need for a

message indicating an unsuccessful transaction (i.e. if said previously acquired security data is not found) ability for the client to address the unsuccessful transactions (e.g. in order to resolve outstanding payments, addressing the account changes and/or discrepancies, etc.).

The examiner points out that generating a message indicating an unsuccessful transaction (e.g. account information invalid) is well known in the art of computing and electronic transactions. Similarly, the mechanisms enabling clients communicating information to address the discrepancies (e.g. credit card information to pay the outstanding payments, update an account information, etc.) are old and well known in the art of computing and electronic transactions (e.g. USPN 6546555, Internet transactions, etc.). Thus, generating a message indicating an unsuccessful transaction and enabling the client to communicating information in order to address an error associated with the transaction (which reads on: if said previously acquired security data is not found, exchanging information associated with the media peripheral, while the media peripheral is located in the home) are obvious variations that are well known in the art. One would have been motivated to use them especially in light of the benefits of these technologies as evidenced by their commercial success. (See KSR ruling).

24. Additionally, as per claim 11, receiving data (e.g. enabling the communication between the headend and the STP) reads on detecting when the media peripheral is communicatively coupled to the node. Alternatively, receiving pockets comprising the security data, which enables to acquire (retrieve) the included security data, also

reads on detecting when the media peripheral is communicatively coupled to the node.

25. As per claims 3, 13 and 20, the data must be read in order to be processed.

26. As per claims 28, although Handelman does explicitly recite that the at least one processor is one of a computer processor, a media peripheral processor, a media exchange system processor or a media processing system it is clear that the processor used in the method disclosed by Handelman not only is utilized by a computer but also handles media exchange transactions, and the examiner points out that assigning a specific name would not affect the functionality of the invention.

27. As per claim 12, Handelman does not explicitly teach that security data and the acquired security data comprise a device identification (ID). However, Handelma's invention is concern with a particular node configuration. Thus, it would have been obvious to an ordinary artisan at the time of applicant's invention to include a device identification in the said security data given the benefit of specifying the type of the device that configuration data is requested and to include the device identification in the previous security data given the benefit of ensuring the correctness of the request.

28. As per claims 7 and 24, the examiner considers validating the data (comparing said security data with the acquired security data) to read on authentication of the data.

29. Although, as per claim 11 and 18, Handelman does not disclose transferring said security data to a media exchange server

30. Claims 5 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Handelman (USPUB 2004/0016002) in view of Stallings (William Stallings, "Network Security Essentials: Applications and Standards", ISBN: 0130160938, 2000). Handelman discloses acquiring the security data and searching for the acquired security data as discussed above.

31. Hadnelman does not disclose authentication the acquired security data. Stallings discloses authentication of the acquired security data (Stallings, MAC and/or Hash, pg. 49-52). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include authentication of the acquired security data as disclosed by Stalling given the benefit of ensuring data integrity.

Conclusion

Although claims 8 and 25 overcame the prior art, the claims are rejected by virtue of their dependence.

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571) 272-3840. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Peter Poltorak/
Examiner, Art Unit 2134

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2136